

Fig. 1

NEW EXTENSION HEADER FIELD NAME	MINIMUM SIZE	FIELD DESIGNATOR
Extension Header Size	128 bits	0 (zero)
Packet Type	2 bits	A
Requested Number of False Packets	8 bits	B
Minimum Hops for False Packets	8 bits	C
Minimum False Packet Body Size (Bytes)	32 bits	D
Maximum False Packet Body size (Bytes)	32 bits	E
Baseline False Packet Body Size (Bytes)	32 bits	F
True Packet (Message) Source Address	128 bits	G
Packet Body Re-encryption Permitted	1 bit	H
False Packet Generation Probability	8 bits	I
False Packet Generation Probability Decay Rate	8 bits	J
Re-encryption Performed	1 bit	K
Re-encryption Probabilty	8 bits	L
Total number of Re-encryp- tions	32 bits	M
Decryption Key Pointer	128 bits per re- encryption	N

Fig. 2

	NEW EXTENSION HEADER FIELD NAME	MEANING	BIT DEFINITIONS
310	Extension Header Size	Size (in bits) of the new extension header within the current packet	N/A
312	Packet Type	Type of packet being transmitted	00 - True packet 01 - First generation false message packet 10 - Second or later generation false message packet. 11 - First generation false message packet generated by an intermediate host between originator and recipient of true message packet
314	Requested Number of False Packets	Number of first generation false packets requested to be generated by true message packet recipient	N/A
316	Minimum Hops for False Packet	Number of laps within the network that a false packet must complete	N/A
318	Minimum False Packet Body Size (Bytes)	Minimal size in bytes of the payload (data segment) in the packet for a false message packet	N/A
320	Maximum False Packet Body size (Bytes)	Maximum size in bytes of the payload (data segment) in the packet for a false message packet	N/A
322	Baseline False Packet Body Size (Bytes)	Actual size in bytes of the payload (data segment) in the true current message packet	N/A

Fig. 3

324	NEW EXTENSION HEADER FIELD NAME	MEANING	BIT DEFINITIONS
	True Packet Source Address	IPv6 address of the source of the true message packet	N/A
326	Re-encryption Permitted	Whether intermediate hosts can add a new level of encryption to packet by re-encrypting the body of the message packet	\emptyset - re-encryption is not permitted 1 - re-encryption is permitted
328	False Packet Generation Probability	Binary value for the false packet generation probability	\emptyset - false packet generation probability is zero > \emptyset - false packet generation probability. Value is equal to 1 divided by the decimalized value of the bit representation
330	False Packet Generation Probability Decay Rate	Binary value for the false packet generation probability decay rate	11111111 - false packet generation probability is set to zero after generating one false packet. <11111111 - bit value to be added to False Packet Generation Probability value each time a false packet is generated at a host
332	Re-encryption Performed	Whether an intermediate host has re-encrypted the packet body	N/A
334	Re-encryption Probability	Binary value for the probability that re-encryption will be performed on the packet	\emptyset - re-encryption probability is zero > \emptyset - re-encryption probability. Value is equal to 1 divided by the decimalized value of the bit representation
336	Total Number of Re-encryptions	A count of the number of re-encryptions performed on a given packet as it moved through the network	N/A
338	Decryption Key Pointer	Designator for each decryption key needed to undo encryption applied by an intermediate host	N/A

Fig. 3A

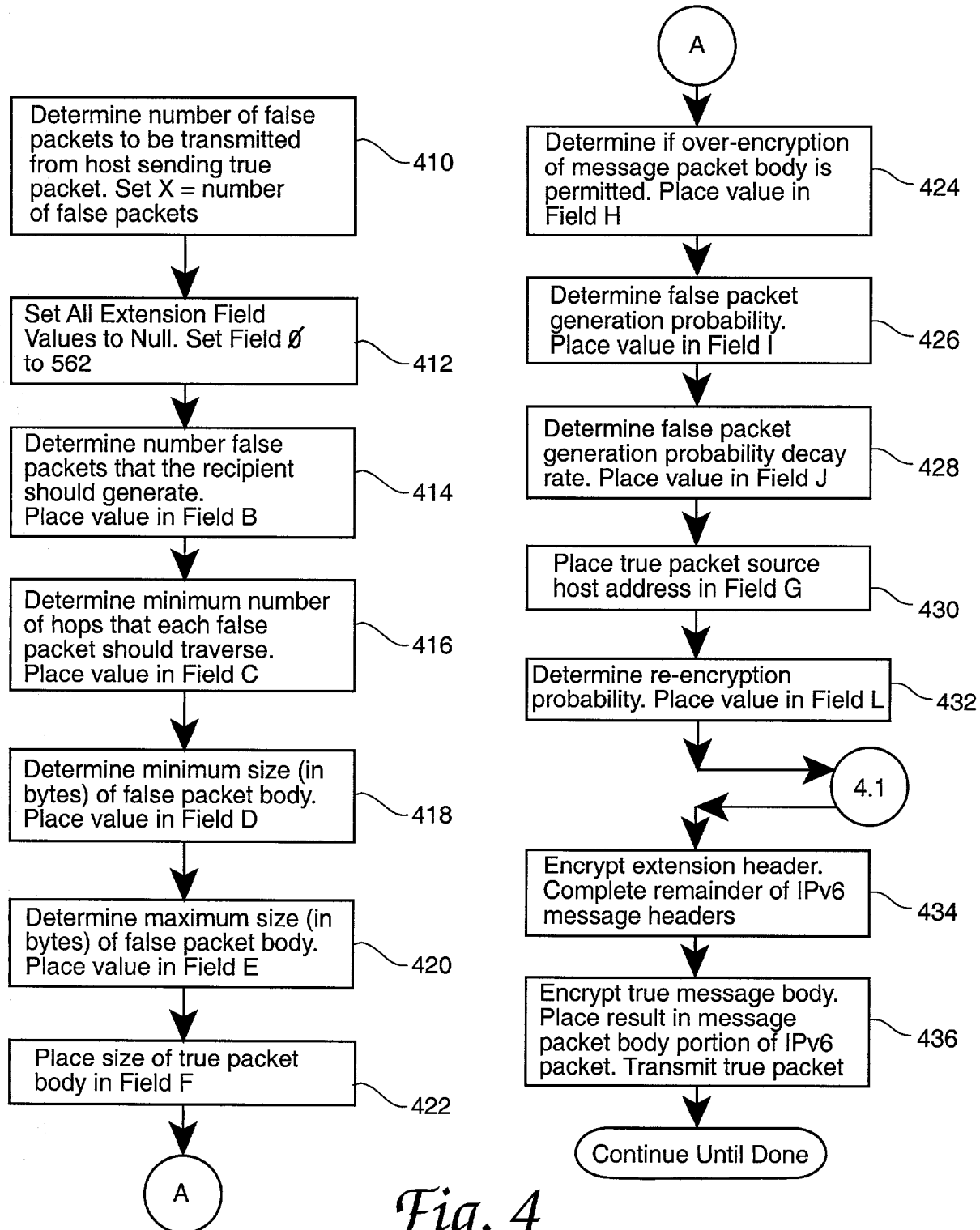


Fig. 4

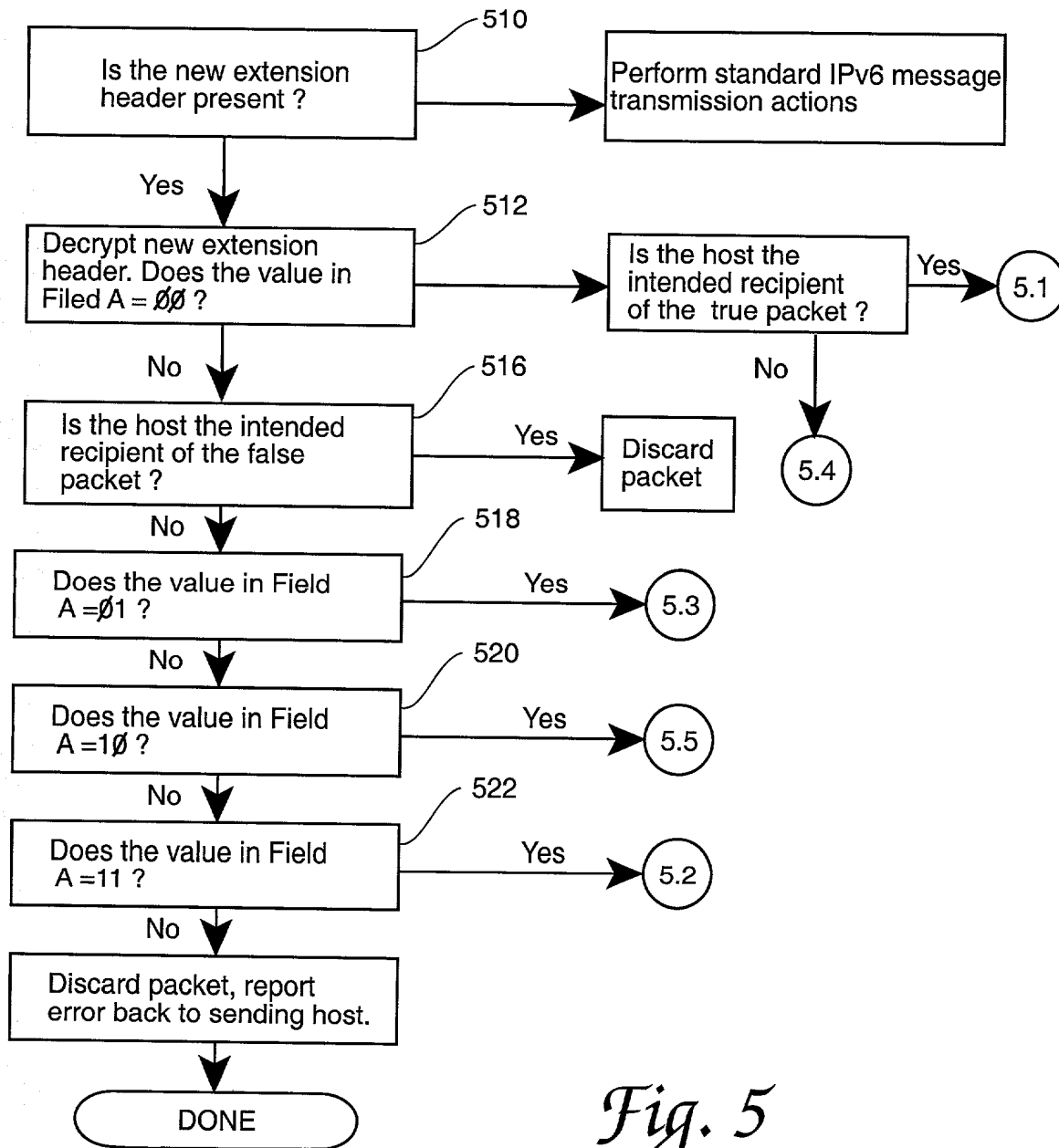


Fig. 5

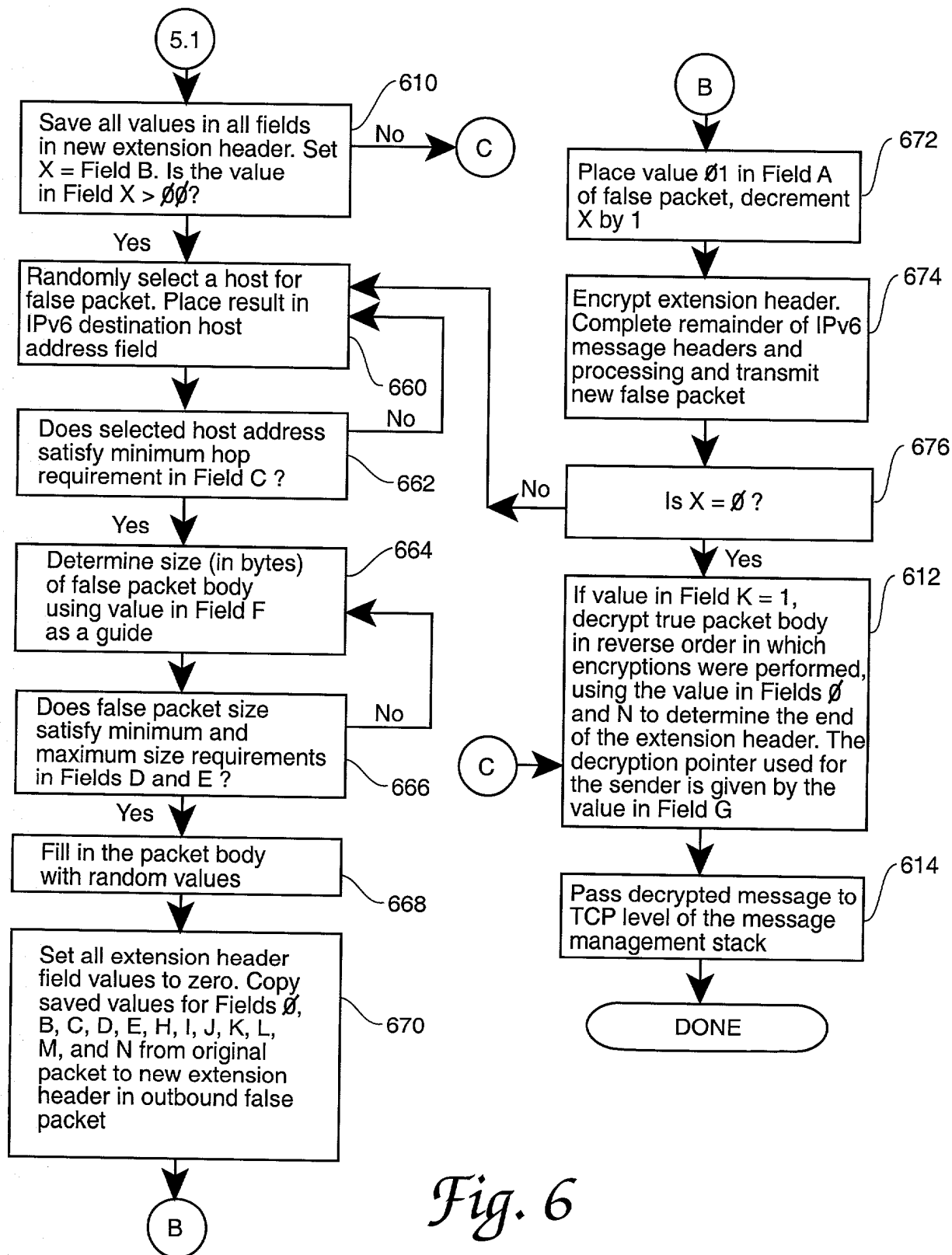


Fig. 6

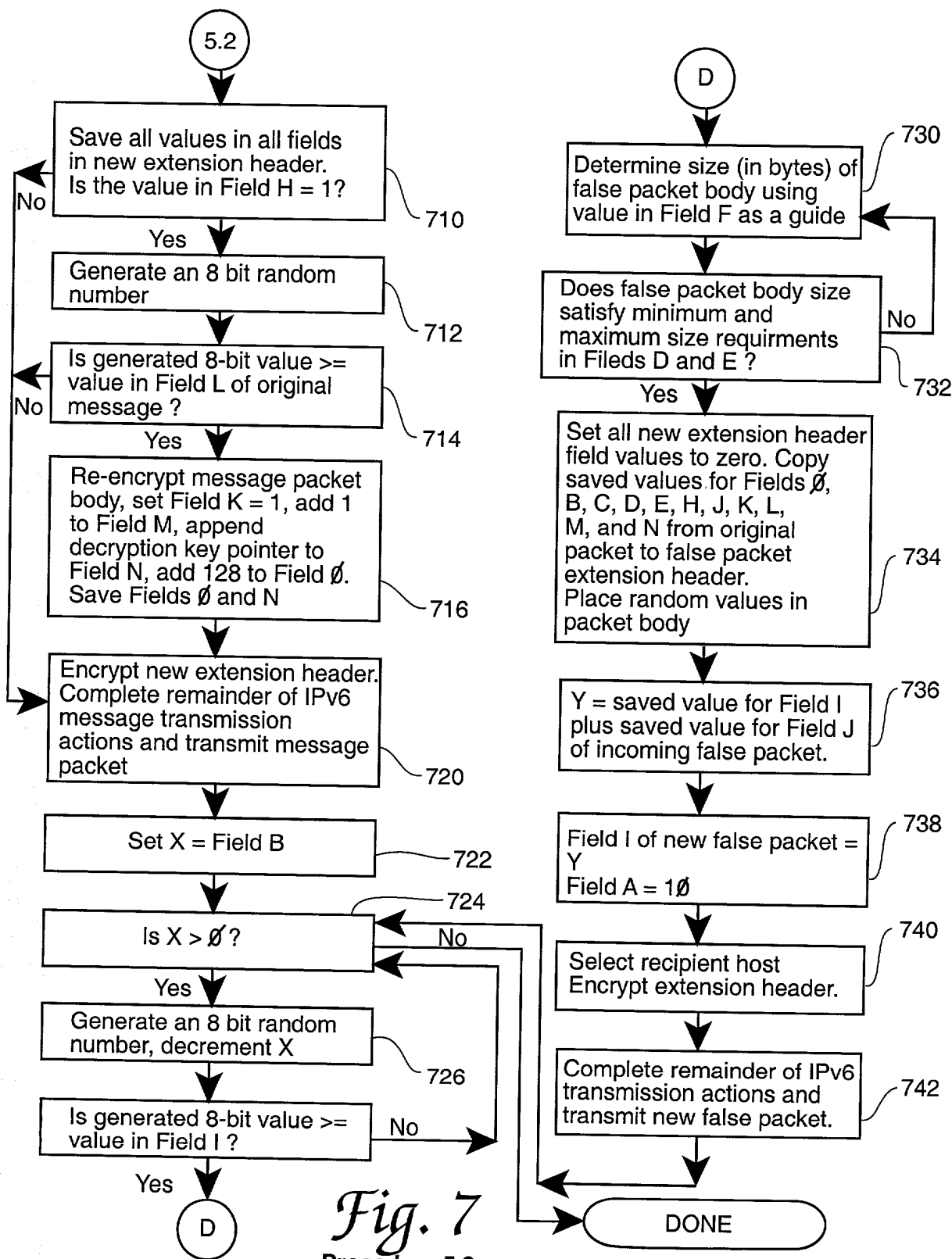
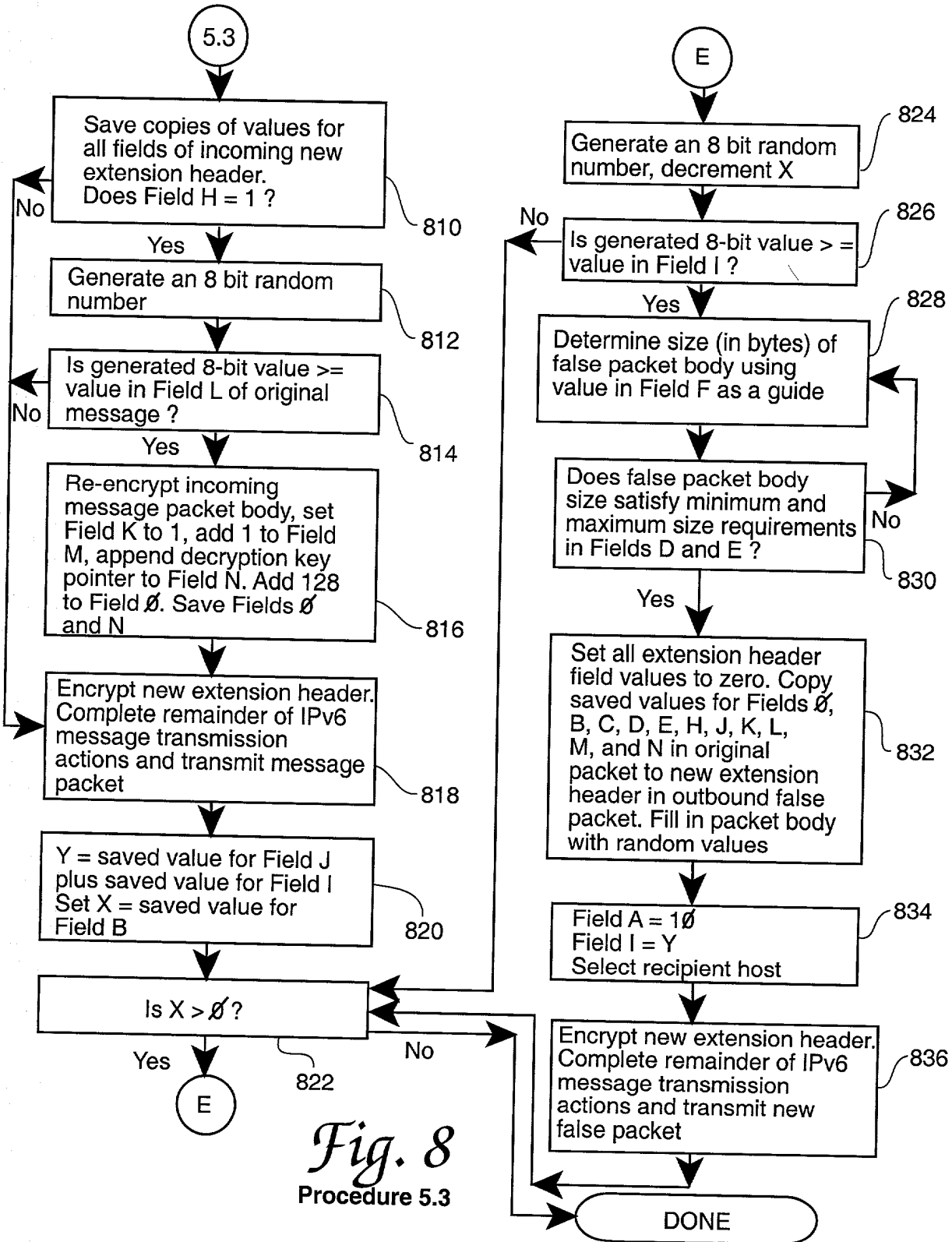


Fig. 7
Procedure 5.2



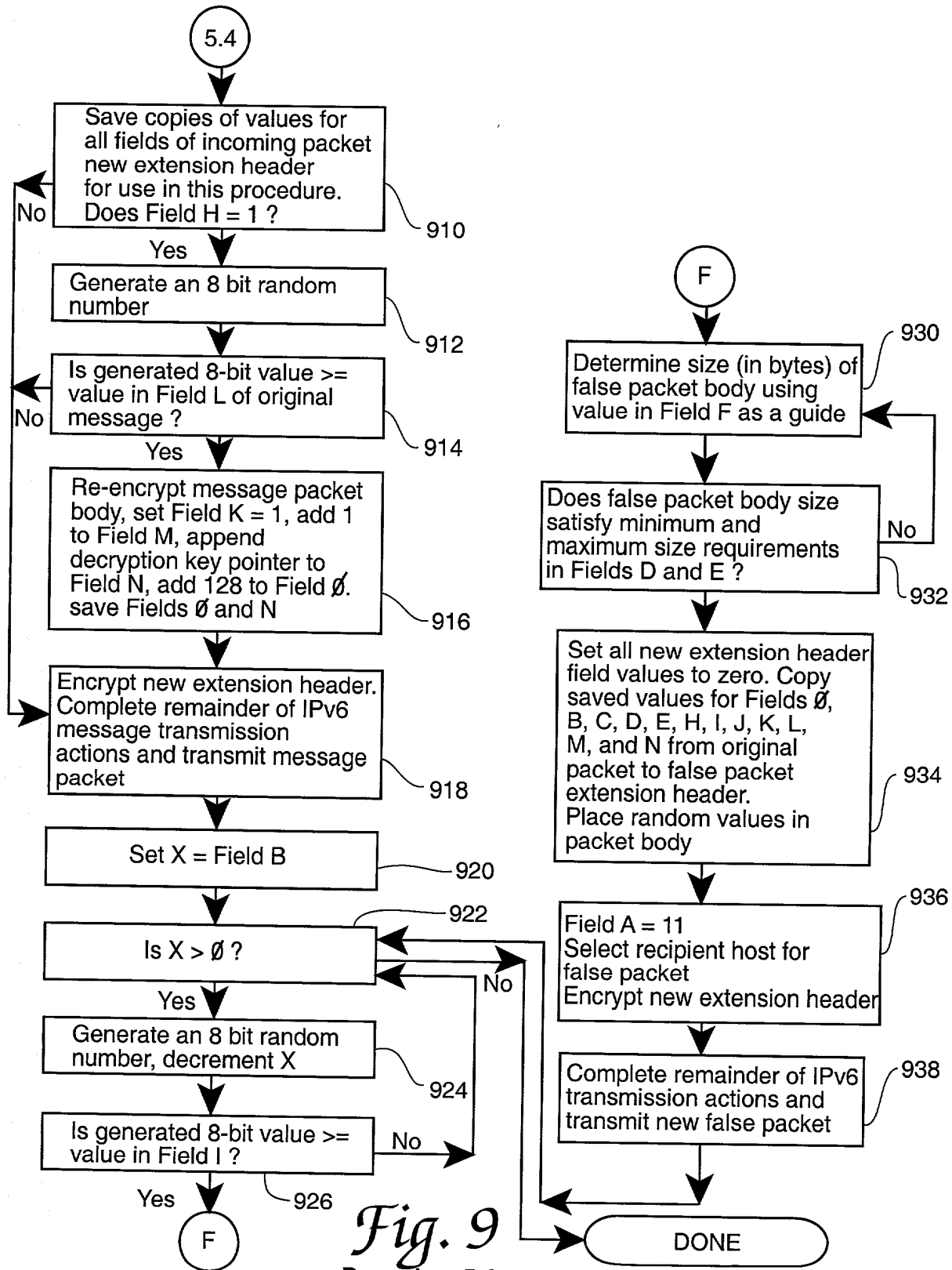


Fig. 9
Procedure 5.4

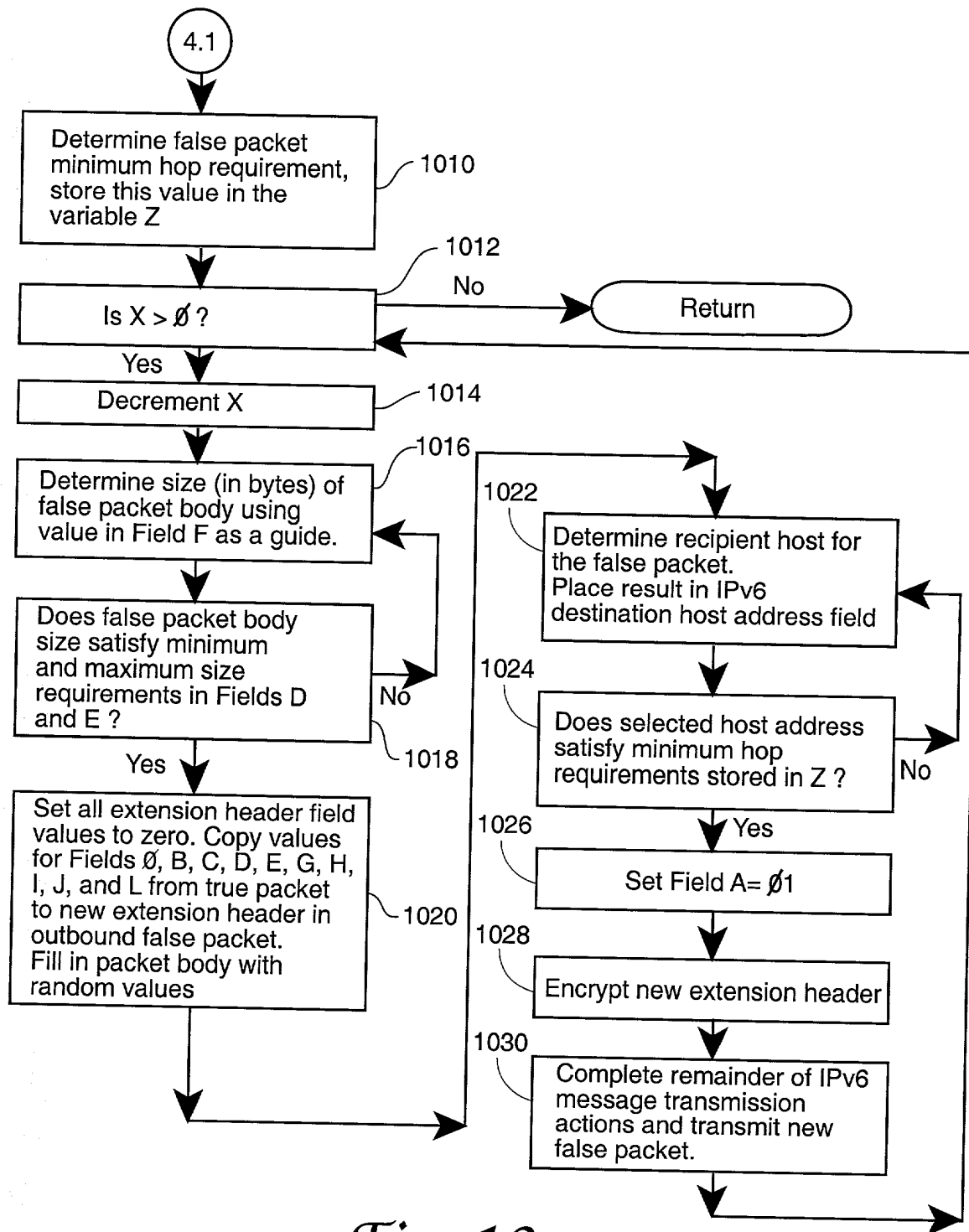


Fig. 10
 Procedure 4.1